IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

ALLIE MCLAUGHLIN, on behalf of herself and all other similarly situated, Plaintiff, v. **FLAGSTAR BANCORP, INC., d/b/a FLAGSTAR BANK**, a Michigan corporation, and **FLAGSTAR BANK, FSB**, a Michigan-based federally chartered bank, Defendants.	Case No. 2:22-cv-11470 **COMPLAINT – CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Allie McLaughlin ("Ms. McLaughlin" or "Plaintiff") brings this action on behalf of herself, and all others similarly situated against Defendant, Flagstar Bancorp, Inc., d/b/a Flagstar Bank and Flagstar Bank, FSB ("Flagstar" or "Defendants"), and their present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and alleges as follows:

INTRODUCTION

1. Flagstar, a Michigan-based full-service bank and mortgage originator with 150 national branches, lost control over at least 1.5 million of its consumers' highly sensitive personal information in a data breach ("Data Breach"), and then failed to adequately notify victims about the breach.

2. On information and belief, the Data Breach occurred between December 3 and 4, 2021. It is unclear when Flagstar first discovered the Data Breach, but on or around June 2, 2022, Flagstar's investigations revealed that cybercriminals gained unauthorized access to consumers' personally identifiable information ("PII") stored on Defendants' network.

3. On information and belief, cybercriminals bypassed Flagstar's inadequate security systems to access consumers' PII in its computer systems.

4. On information and belief, Flagstar suffered a previous data security breach in late

2020[1] and has failed to implement the necessary security safeguards to protect its consumers' PII.

5. On information and belief, the stolen PII included, at least, consumers' names, Social Security numbers, addresses, Tax ID numbers, dates of birth, and financial account information and numbers.

6. On or around June 17, 2022—over six months after the Data Breach first occurred—Flagstar finally began notifying victims about the breach (the "Breach Notice").[2]

7. Flagstar's Breach Notice obfuscated the nature of the breach and the threat it posed—refusing to tell its consumers how many people were impacted, how the breach happened, or why it took so long for Flagstar to discover that hackers had gained access to highly sensitive consumer information.

8. Worse yet, the Breach Notice deliberately underplayed the breach's severity and misrepresented that "[Flagstar has] no evidence that any of the information has been misused," even though Flagstar knew cybercriminals had infiltrated its systems and stolen highly sensitive nonpublic information. Exh. A.

9. Flagstar's failure to timely detect and report the Data Breach made its consumers vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

10. Flagstar knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

11. In failing to adequately protect consumers' information, adequately notify them

---

[1] *See* Flagstar Bank hit by data breach exposing customer, employee data, https://www.bleepingcomputer.com/news/security/flagstar-bank-hit-by-data-breach-exposing-customer-employee-data/ (last visited June 29, 2022).

[2] A true and accurate copy of Flagstar's Breach Notice is attached to this Complaint as **Exhibit A**. Breach Notice obtained from the website of the office of the Maine Attorney General, https://apps.web.maine.gov/online/aeviewer/ME/40/667f2112-b49f-445d-be03-dee38e32bf8e.shtml (last visited June 29, 2022).

about the breach, and misrepresenting the nature of the breach, Flagstar violated state and federal law and harmed at least 1.5 million of its consumers.

12. Plaintiff and members of the proposed Class are victims of Defendants' negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendants with their PII. But Defendants betrayed that trust. Defendants failed to properly use up-to-date security practices to prevent the Data Breach.

13. Plaintiff McLaughlin obtained a mortgage from Flagstar in March 2020 and became a victim of Defendants' negligence and insufficient data security practices when her PII was accessed and stolen in the Data Breach. Plaintiff has suffered a tangible and concrete injury-in-fact.

14. Accordingly, Plaintiff, on her own behalf and on behalf of a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendants' possession.

THE PARTIES

15. Plaintiff, Allie McLaughlin, is a natural person and citizen of Washington state, residing in Pasco, Washington, where she intends to remain. Ms. McLaughlin is a current Flagstar consumer and Data Breach victim, receiving Flagstar's Breach Notice in late-June 2022.

16. Defendant, Flagstar Bancorp, Inc., is a corporation organized under the laws of Michigan with its principal place of business at 5151 Corporate Drive, Troy, MI 48098.

17. Defendant, Flagstar Bank, FSB, is a federally chartered bank headquartered in and with its principal place of business in Troy, MI.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

19. This Court has personal jurisdiction over Defendants because Flagstar is headquartered in this District and Flagstar conducts substantial business in this District.

20. Venue is proper in this District because Flagstar is headquartered in this District and a substantial part of the events or omissions giving rise to Ms. McLaughlin's claims occurred in this District.

BACKGROUND FACTS

a. Flagstar

21. According to its website, Flagstar is a full-service bank and the sixth largest bank mortgage originator in the country.[3]

22. On information and belief, Flagstar accumulates and manages highly sensitive PII of consumers through its banking and mortgage financing services.

23. Despite recognizing its duty to do so, on information and belief, Flagstar has not implemented reasonable cybersecurity safeguards or policies to protect consumer PII, or trained its employees to prevent, detect, and stop data breaches of Flagstar's systems. As a result, Flagstar leaves vulnerabilities in its systems for cybercriminals to exploit and gain access to consumer PII.

24. On information and belief, Flagstar has failed to implement adequate security measures despite experiencing a similar data breach in December 2020.

b. Flagstar Fails to Safeguard Consumers' PII

25. Plaintiff and the proposed Class are consumers whose PII was maintained in Flagstar's files and systems.

26. On information and belief, Flagstar collects and maintains PII in its systems for ordinary banking purposes, as well as for purposes of processing consumers' mortgage and/or refinancing applications.

27. In collecting and maintaining the consumer PII, Flagstar implicitly agrees it will

[3] *See* Flagstar's website: https://www.flagstar.com/about-flagstar.html (last visited June 29, 2022).

safeguard the data using reasonable means according to its internal policies and federal law.

28. In fact, Flagstar informs consumers that it collects and maintains their PII through the Privacy Policy (the "Privacy Policy").[4]

29. The Privacy Policy warrants that Flagstar "use[s] security measures that comply with federal law" to protect consumers' PII from "unauthorized access and use[.]" Exh. B. Notably, the Privacy Policy states that even when consumers "are *no longer* [Flagstar's] customer, [Flagstar] continue[s] to share [consumers'] information as described in [its Privacy Policy]." Put differently, Flagstar admits to maintaining and sharing consumers' PII indefinitely.

30. Flagstar represented to consumers and its mortgage applicants that their PII would be secure. Plaintiff and the proposed Class relied on such representations when they agreed to provide their PII and transact with Flagstar.

31. Consumers place value in data privacy and security. These are important considerations when deciding who to do business with. Plaintiff would not have transacted with, nor provided her PII to, Flagstar had she known that Flagstar does not take all necessary precautions to secure the personal and financial data given to it by consumers.

32. Despite its duties and alleged commitments to safeguard PII, Flagstar does not follow industry standard practices in securing consumers' PII.

33. In December 2021, cybercriminals bypassed Flagstar's inadequate security systems undetected and gained unfettered accessed consumers' PII.

34. However, it was not until June 2022 that Flagstar finally determined that cybercriminals had accessed consumers' PII during the December 2021 breach.

35. In response to the Data Breach, Flagstar contends that it "promptly took steps to secure its environment[.]" Exh. A. Although Flagstar fails to expand on these alleged "steps to secure its environment," such measures should have been in place *before* the Data Breach.

---

[4] *See* Flagstar's website: https://www.flagstar.com/content/dam/flagstar/pdfs/about-flagstar/PrivacyPolicy.pdf (last visited June 29, 2022). A true and accurate copy of the Privacy Policy is attached to this Complaint as **Exhibit B.**

36. Through its Breach Notice, Flagstar also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "always remain vigilant in reviewing [their] financial account statements and credit reports for fraudulent or irregular activity on a regular basis." Exh. A.

37. Flagstar has offered two years of complimentary identity monitoring services to victims, which does not adequately address the lifelong harm that consumers will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers and birth dates. Further, the breach exposed consumers' nonpublic financial information, a disturbing harm in and of itself.

38. Even with complimentary identity-theft protection, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

39. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

40. On information and belief, Flagstar failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over consumer PII. Flagstar's negligence is evidenced by its failures to prevent the Data Breach, stop cybercriminals from accessing PII, and notably, to timely detect that certain PII was compromised and stolen after beginning its "investigations."

c. Plaintiff's Experience

41. Plaintiff McLaughlin is a Washington state citizen. She applied for and was approved for a residential mortgage through Flagstar in March 2020.

42. To complete her mortgage application process and obtain lender approval, Plaintiff was required to provide her PII to Flagstar and trusted Flagstar would use reasonable measures to

protect it according to Flagstar's internal policies, as well as state and federal law.

43. Plaintiff has and will spend considerable time and effort monitoring her accounts to protect herself from identity theft. She fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

d. Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

44. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendants.

45. The ramifications of Flagstar's failure to keep Plaintiff's and the Class's PII secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, or other nonpublic financial information, without permission, to commit fraud or other crimes.

46. As a result of Flagstar's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in its possession.

47. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.[5]

48. The value of Plaintiff's and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

49. It can take victims years to stop identity or PII theft, giving criminals time to sell that information for cash.

50. One such example of criminals using PII for profit is the development of "Fullz" packages.

51. Cybercriminals can cross-reference multiple sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.[6]

52. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain

[5] *See* Here's How Much Your Personal Information Is Selling for on the Dark Web, Experian, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited June 29, 2022).

[6] *Id.*

information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

53. Defendants disclosed the PII of Plaintiff and members of the proposed Class's for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (*i.e.*, identity fraud), all using the stolen PII.

54. Flagstar's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PII of Plaintiff and members of the proposed Class to unscrupulous operators, con artists, and criminals.

55. Further, Flagstar's failure to learn from its previous December 2020 data breach demonstrates its nonchalant approach to cybersecurity and its institutional disregard for consumer data protection.

56. Defendants' failure to properly notify Plaintiff and members of the proposed Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

e. Flagstar Failed to Adhere to FTC Guidelines

57. According to the Federal Trade Commission ("FTC"), the need for data security

should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Flagstar, should employ to protect against the unlawful exposure of PII.

58. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

59. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

60. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. Flagstar's failure to employ reasonable and appropriate measures to protect against unauthorized access to consumers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

CLASS ACTION ALLEGATIONS

63. Plaintiff brings this action pursuant to Federal Rule of Civil Procedure 23 and MCR 3.501 on behalf of herself and all members of the proposes classes (together the "Class"), defined as follows:

> **Nationwide Class:** All individuals residing in the United States whose personal information was compromised in the Data Breach disclosed by Flagstar in June 2022.
>
> **Washington Subclass:** All individuals residing in the State of Washington whose personal information was compromised in the Data Breach disclosed by Flagstar in June 2022.

64. The following people are excluded from the Class: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which the Defendants or its parent has a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendants' counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

65. Plaintiff reserves the right to amend the Class definition or add a Class if further information and discovery indicate that other classes should be added and if the definition of the Class should be narrowed, expanded, or otherwise modified.

66. Plaintiff and members of the Class satisfy the numerosity, commonality, typicality, and adequacy requirements under Fed. R. Civ. P. 23:

a. **Numerosity**: The exact number of Class members is unknown but is estimated to be up to 1,547,169 persons at this time, and individual joinder in this case is impracticable. Class Members can be easily identified through Defendants' records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach,

consumer breach of contract, unlawful trade practices, and class action controversies;

b. **Typicality**: Plaintiff's claims are typical of the claims of other Class members in that Plaintiff, and the Class Members sustained damages arising out of Defendants' Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and the Class Members sustained similar injuries and damages, as a result of Defendants' uniform illegal conduct;

c. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Class, and Defendants have no defenses unique to Plaintiff;

d. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

i. whether Defendants violated the laws asserted herein, and other statutory privacy and consumer protection laws;

ii. Whether Defendants had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

iii. whether Defendants breached the duty to use reasonable care to safeguard Plaintiff's and the Class's PII;

iv. Whether Defendants breached their contractual promises to safeguard Plaintiff's and the Class's PII;

v. whether Defendants knew or should have known their practices and representations related to the Data Breach, and PII were deceptive and unfair;

vi. whether Defendants knew or should have known about the inadequacies

of their data security policies and system and the dangers associated with storing sensitive PII;

vii. whether Defendants failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized release and disclosure;

viii. whether the proper data security measures, policies, procedures and protocols were in place and operational within Defendants' computer and software systems to safeguard and protect Plaintiff's and the other Class Members' PII from unauthorized release and disclosure;

ix. whether Defendants took reasonable measures to determine the extent of the Data Breach after it was discovered;

x. whether Defendants' delay in informing Plaintiff and the Class of the Data Breach was unreasonable;

xi. whether Defendants' method of informing Plaintiff and the Class of the Data Breach was unreasonable;

xii. whether Defendants' conduct was deceptive, unfair, or unconscionable, or constituted unfair competition;

xiii. whether Defendants' conduct was likely to deceive the public;

xiv. whether Defendants are liable for negligence or gross negligence;

xv. whether Defendants' conduct, practices, statements, and representations about the Data Breach of the PII violated applicable state laws;

xvi. whether Defendants knew or should have known their representations were false, deceptive, unfair, and misleading;

xvii. whether Plaintiff and the Class were injured as a proximate cause or result of the Data Breach;

xviii. whether Plaintiff and the Class were damaged as a proximate cause or result of Defendants' breach of their contract with Plaintiff and the Class;

xix. whether Defendants' practices and representations related to the Data Breach that compromised the PII breached implied warranties;

xx. what the proper measure of damages is; and

xxi. whether Plaintiff and the Class Members are entitled to restitutionary, injunctive, declaratory, or other relief.

e. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Class will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for the individual members of the Class to obtain effective relief from Defendants' misconduct. Even if members of the Class could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort and expense will be fostered, and uniformity of decisions ensured.

COUNT I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

67. Plaintiff and the members of the Nationwide Class incorporate the above allegations as if fully set forth herein.

68. Plaintiff and members of the Class entrusted their PII to Defendants. Defendants owed to Plaintiff and other members of the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and

unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

69. Defendants owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards for data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII by disclosing and allowing access to consumers' PII to unknown third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who made that happen.

70. Defendants owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. These duties are required and necessary for Plaintiff and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

71. Defendants owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security protocols. Plaintiff and members of the Class were required to provide their personal information to Defendants in order to complete and obtain approval for their mortgages, or to obtain access to other banking services, such as establishing savings/checking accounts, obtaining personal or business loans, and/or obtaining credit cards through the Defendants. According to their Privacy Policy, Defendants retained and shared this sensitive information, even after the parties' business-consumer relationship ended.

72. The risk that unauthorized persons would try to gain access to the PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII, it was inevitable that

unauthorized individuals would try to access Defendants' databases containing the PII—whether by malware or otherwise.

73. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and members of the Class and the importance of exercising reasonable care in handling it.

74. Defendants breached their duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and the other Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

75. Defendants' breach of their common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

76. Plaintiff and the members of the Nationwide Class incorporate the above allegations as if fully set forth herein.

77. Defendants offered to provide banking and residential financing services to Plaintiff and members of the Class in exchange for payment. Plaintiff and the Class accepted Defendants' offer and paid certain fees and costs associated with setting up bank accounts, or obtaining mortgages and other loan services.

78. Defendants required Plaintiff and members of the Class to provide their PII, including, but not limited to, names, Social Security numbers, addresses, Tax ID numbers, dates of birth, income information, and financial account information in order to receive the services offered by the Defendants.

79. Plaintiff and members of the Class exchanged valuable consideration – money – with Defendants for banking and loan services, a crucial part of which was Defendants' implicit promise to protect their PII from unauthorized disclosure.

80. In their Privacy Policy, Defendants expressly promised Plaintiff and the Class that Defendants would only disclose (share) PII under certain circumstances, none of which relate to the Data Breach.

81. Necessarily implicit in the agreement(s) between Defendants and their consumers, including Plaintiff and members of the Class, was Defendants' obligation to use such PII for its "everyday business purposes" and "marketing purposes" only, to take reasonable steps to secure and safeguard that PII, and not make disclosures of the PII to unauthorized third parties.

82. Further implicit in the agreement, Defendants were obligated to provide Plaintiff and members of the Class with prompt and adequate notice of any and all unauthorized access and/or theft of their PII.

83. Plaintiff and members of the Class would not have entrusted their sensitive PII to Defendants in the absence of such agreement with Defendants.

84. Defendants materially breached the implied contract(s) they had entered with Plaintiff and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information.

85. The damages sustained by Plaintiff and members of the Class as described above

were the direct and proximate result of Defendants' material breaches of its agreements.

86. Plaintiff and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendants.

87. The covenant of good faith and fair dealing is an element in every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

88. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

89. Defendants failed to promptly advise Plaintiff and members of the Class of the Data Breach.

90. In these and other ways, Defendants violated its duty of good faith and fair dealing.

91. Plaintiff and members of the Class have sustained damages as a result of Defendants' breaches of their agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

92. Plaintiff, on behalf of herself and the Class, seeks compensatory damages for breach of implied contract, which includes the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and the Nationwide Class)

93. Plaintiff and the members of the Nationwide Class incorporate the above allegations as if fully set forth herein.

94. Defendants publicized private details and facts not generally known to the public, not publicly available, and not of legitimate public concern about Plaintiff and the Class by disclosing and exposing Plaintiff's and Class's PII to enough people that it is reasonably likely those facts will become known to the public at large, including without limitation on the dark web and elsewhere.

95. Plaintiff and members of the Class had a legitimate expectation of privacy regarding their highly sensitive financial and personal information and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

96. Defendants owed a duty to consumers, including Plaintiff and the Class, to keep this information confidential.

97. The disclosure of the PII, including consumers' names, Social Security numbers, Tax ID numbers, addresses, dates of birth, and financial account and/or payment card information is particularly harmful and would be offensive to a reasonable person of ordinary sensibilities.

98. Defendants have extensive knowledge of their consumers' financial standings and therefore has a special relationship with Plaintiff and the Class and Defendants' disclosure of PII is certain to embarrass them and offend their dignity. Defendants should appreciate that the cyber-criminals who stole the PII would further sell and disclose the PII as they are doing. That the original disclosure is devastating to the Plaintiff and the Class, even though it originally may have only been disclosed to one person or a limited number of cyber-criminals, does not render it any less a disclosure to the public-at-large.

99. Defendants acted with a knowing state of mind when they permitted the Data Breach because they knew their information security practices were inadequate.

100. Defendants acted with a knowing state of mind when they failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

101. Acting with knowledge, Defendants had notice and knew that their inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

102. As a proximate result of Defendants' acts and omissions, the private and sensitive PII of Plaintiff and the Class were stolen by a third party and is now available to disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

103. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since those personal and financial records are still maintained by Defendants with their inadequate cybersecurity system and policies.

104. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard the records of Plaintiff and the Class. In addition to injunctive relief, Plaintiff, on behalf of herself and the other members of the Class, also seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV
Violation of the Washington Consumer Protection Act, RCW § 19.86, *et seq.*
(On Behalf of the Plaintiff and the Washington Subclass)

105. Plaintiff and the members of the Washington Subclass incorporate the above allegations as if fully set forth herein.

106. Each Defendant is a "person" under the Washington Consumer Protection Act, RCW § 19.86.101(1), and they conduct "trade" and "commerce" under RCW § 19.86.010(2).

107. Plaintiff and other members of the proposed Washington Subclass are "persons" under RCW § 19.86.010(1).

108. Defendants' failure to safeguard the PII exposed in the Data Breach constitutes an unfair act that offends public policy.

109. Defendants' failure to safeguard the PII compromised in the Data Breach caused

Plaintiff and the proposed Washington Subclass substantial injury. Defendants' failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

110. Defendants' failure to safeguard the PII disclosed in the Data Breach, and its failure to give time and complete notice of the Data Breach to victims, is unfair because these acts and practices are immoral, unethical, oppressive, and unscrupulous.

111. Defendants' unfair acts or practices occurred in its trade or business and have injured and can injure a substantial portion of the public. Defendants' general conduct as alleged injures the public interest, and the acts Plaintiff complains of are ongoing and have a substantial likelihood of being repeated.

112. As a direct and proximate result of Defendants' unfair acts or practices, Plaintiff and the proposed Washington Subclass suffered an injury in fact.

113. As a result of Defendants' conduct, Plaintiff and members of the Washington Subclass's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' conduct, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

114. Plaintiff and the proposed Washington Subclass are entitled to an order enjoining the conduct complained of and ordering Defendants to take remedial measures to prevent similar data breaches; actual damages; treble damages under § 19.86.090; and the costs of bringing this suit, including reasonable attorney fees.

COUNT V
Violation of the Washington Data Breach Disclosure Law
(On Behalf of the Plaintiff and the Washington Subclass)

115. Plaintiff and the members of Washington Subclass incorporate the above allegations as if fully set forth herein.

116. RCW § 19.255.010(2) provides that "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

117. The Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendants, leading to a "breach of the security of [Defendants'] systems," as defined by RCW § 19.255.010.

118. Defendants failed to disclose that the PII of at least 34,026 of its Washington consumers had been compromised "immediately" upon discovery, and in doing so unreasonably delayed informing Plaintiff and the proposed Washington Subclass about the Data Breach.

119. A violation under RCW § 19.255 is an unfair or deceptive act in trade or commerce and an unfair method of competition for purposes of applying the consumer protection act under § 19.86.

PRAYER FOR RELIEF

Plaintiff and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representatives, and appointing their counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

RESPECTFULLY SUBMITTED AND DATED this 29th day of June, 2022.

/s/ Nathan J. Fink
FINK BRESSACK
Nathan J. Fink (P75185)
38500 Woodward Ave, Suite 350
Bloomfield Hills, MI 48304
Telephone: (248) 971-2500
nfink@finkbressack.com

Samuel Strauss
Raina Borrelli
TURKE & STRAUSS, LLP
613 Williamson Street, Suite 201
Madison, WI 53703
Telephone: (608) 237-1775
Sam@turkestrauss.com
Raina@turkestrauss.com

Counsel for Plaintiff and the Proposed Class